カスペルスキーAPTインテリジェンスレポート

kaspersky BRING ON THE FUTURE

カスペルスキーAPTインテリジェンスレポート

カスペルスキーのAPTインテリジェンスレポートのお客様は、弊社が実施した調査結果および確認された情報（確認されたすべてのAPTの完全な技術データ（さまざまな形式）や、公表されない脅威に関するデータなど）に継続的にアクセスすることができます。レポートにはエグゼクティブサマリーが含まれており、経営幹部レベル向けのわかりやすい情報を提供します。関連するAPTを説明し、関連するIOCとYARAルールを含むAPTの詳細な技術説明も含まれています。これにより、セキュリティリサーチャー、マルウェアアナリスト、セキュリティエンジニア、ネットワークセキュリティアナリスト、およびAPTリサーチャーに脅威に対してすばやく正確に対応できる実用的なデータを提供できます。

弊社の専門家は、サイバー犯罪グループの戦術で検知した変化を直ちにお客様に通知します。セキュリティ防御におけるさらなる強力な調査および分析コンポーネントであるKasperskyの完全なAPTレポートデータベースにもアクセスできます。

メリット

MITRE ATT&CK
レポートで説明されているすべてのTTPsは、MITRE ATT&CKにマッピングされ、対応するセキュリティ監視のユースケースを開発して優先順位を付け、ギャップ分析を実行し、関連するTTPsに対する現在の防御をテストすることで、検知と応答を向上させることができます。

非公開APTの情報
さまざまな理由により、すべての有名な脅威が既知になっているとは限りません。しかし、弊社はそれらすべての脅威をお客様と共有します。

権限付きアクセス
一般公開する前に、調査中に最新の脅威に関する技術的説明を受信

遡及的分析
サブスクリプション中は、以前発行されたすべてのプライベートレポートにアクセスできます。

技術データへのアクセス
openIOCやSTIXなどの標準的な形式で使用可能なIOCの詳細なリスト、および弊社のYARAルールへのアクセスを含む

攻撃者のプロファイル
発生源となる疑わしい国と主なアクティビティ、使用されたマルウェアファミリー、対象となる産業と地域、使用されたすべてのTTPsの説明（MITRE ATT&CKへのマッピングあり）を含む

継続的なAPT活動のモニタリング
APT配信の情報、IOC、コマンド&コントロール用インフラなどの調査中に、実用的な情報にアクセス可能

RESTful API
セキュリティワークフローのシームレスな統合と自動化

www.kaspersky.co.jp